are independent of the in-channel power levels. For harmonic and unwanted emissions that are independent of the in-channel power (e.g., a fixed field strength level), NTIA recommends that the limits specified in Sections 15.247 and 15.249 be applied for the higher-powered unlicensed devices as proposed by the Commission. For higher-powered unlicensed devices where the unwanted emissions are dependent on the in-channel power level, the unwanted emission limit should be reduced commensurate with the increase in the in-channel power level. In the Commission's proposal, this would result in a reduction of 8 dB in the unwanted emission levels for the higher-powered devices.

VI. GEO-LOCATION TECHNOLOGIES USED IN CONJUNCTION WITH AN ON-LINE DATABASE HOLDS PROMISE FOR SHARING BETWEEN UNLICENSED DEVICES AND RADIO SERVICES USING RECEIVERS AT FIXED LOCATIONS.

The Commission seeks comment on the positional accuracy necessary if geo-location technology such as the Global Positioning System (GPS) were used. Related to CR geo-location techniques, the Commission also requests comment on how a device using geo-location would access a table or database showing where operation is permitted; who would be responsible for maintaining the database; should the geo-location technology be required to be incorporated within the device; and how would the device react if it were unable to determine its position within a specified accuracy limit.[26]

The positional accuracy of different GPS receiver architectures is discussed in Appendix C. The Commission adopted accuracy and reliability requirements for Automatic Location Identification as part of its Rules for wireless carrier enhanced 911 (E911) service.[27] The

26. Cognitive Radio NPRM at ¶ 47.

27. *Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, Third Report and Order, CC Docket No. 94-102, 14 F.C.C. Rcd. 17388 (1999).

accuracy and reliability requirements for E911 Phase II operations for handset-based solutions are 50 meters for 67 percent of calls, 150 meters for 95 percent of the calls. NTIA recommends that the Commission adopt positional accuracy requirements for CR devices employing geo-location capabilities that are at least as stringent as the E911 requirements. Many manufacturers are developing GPS chipsets to meet the Commission's December 31, 2005 Phase II deadline, so the technology should be available at a reasonable cost. The Commission's Office of Engineering and Technology has also developed guidelines for testing and verifying these positional accuracy requirements.[28]

In comments filed in response to another rulemaking proceeding, the Institute of Electrical and Electronics Engineers (IEEE) 820.18 Radio Regulatory Technical Advisory Group stated that embedding GPS technology in unlicensed devices is technically feasible and could be used to limit the device so it does not transmit when located in or near an area where interference to a fixed receiver is likely.[29] NTIA agrees with the IEEE that unlicensed devices that employ GPS technology in conjunction with an on-line database of the fixed site locations can be used to prohibit that device from operating in those areas.[30] Issues related to the implementation of geo-location techniques and the on-line database are discussed in Appendix C.

NTIA also agrees with the IEEE that it is feasible to incorporate GPS chipsets within unlicensed devices. As discussed earlier, GPS chipsets are being incorporated in handsets to meet the Commission's E911 mandate. Incorporating the geo-location hardware in the

---

28. Federal Communications Commission, OET Bulletin No. 71, *Guidelines for Testing and Verifying the Accuracy of Wireless E911 Location Systems* (April 12, 2000).

29. Institute of Electrical and Electronics Engineers Comments, ET Docket No. 02-380, at 10 (April 17, 2003).

30. The exclusion areas where unlicensed device operation is prohibited would be determined based on the characteristics and operational scenarios for the licensed service and the unlicensed devices.

unlicensed device is the only practical way from an interference protection standpoint to effectively implement geo-location technology. NTIA recommends that if the Commission permits geo-location technology to facilitate sharing with other fixed receivers, the position location technology should be incorporated within the unlicensed device.

GPS signal failures can occur in urban canyons, indoors, or in shaded areas where the received signals are too noisy, too attenuated or distorted by multipath to be received and used reliably in ranging. Under such conditions, demodulating the navigation data included in the satellite broadcast becomes practically impossible.[31] Appendix C describes a technology that can be deployed to compensate for losses in the satellite signal. The time between when this momentary loss of satellite signals occurs and when the receiver can no longer provide position information depends on the GPS receiver architecture, application, and manufacturer implementation. Since unlicensed devices that employ geo-location techniques require a position location to control device transmissions, it is important to determine how much time should be permitted after the position location is lost and when the device must cease all transmissions. Appendix C shows that using 60 seconds after position information is no longer available as the upper limit for unlicensed devices employing geo-location techniques to cease transmissions seems reasonable. However, larger separation distances between unlicensed devices and the fixed receivers could accommodate longer periods of time when the geo-location capability is not available.

NTIA believes that geo-location technology used in conjunction with an on-line database of sites that require protection holds promise for facilitating sharing between unlicensed devices and radio services using receivers at fixed locations. NTIA believes that GPS-based technology

31. A minimum of three to four satellites are necessary for a GPS receiver to determine a position location.

incorporated within the unlicensed device is capable of providing position locations with the necessary accuracy. However, many issues related to the accuracy and integrity of the on-line database as well as the integrity of the data downloaded to the unlicensed device must be addressed. If the geo-location device is unable to obtain a location, or the database is not successfully downloaded, the unlicensed device should not be permitted to transmit. In a separate rulemaking, the Commission is proposing to implement geo-location techniques to permit sharing between unlicensed devices and fixed-satellite earth station and radar receivers operating in the 3650-3700 MHz band. NTIA believes that the experience gained with implementing geo-location technology in the 3650-3700 MHz band can be used to address the issues related to the unlicensed device interface with the on-line database.

VII. TECHNICAL, COST, AND LEGAL ISSUES, NOT THE COMMISSION'S RULES ARE LIMITING THE IMPLEMENTATION OF SOFTWARE DEFINED RADIO AS A POTENTIAL SOLUTION TO THE PUBLIC SAFETY INTEROPERABILITY PROBLEM.

The Commission seeks comment on how CR technologies can facilitate interoperability between systems. Specifically, the Commission seeks comment on any rule changes necessary to take advantage of these benefits for interoperability between systems.[32]

The Public Safety Wireless Advisory Committee (PSWAC) Final Report defines interoperability as the ability of two or more public safety communications systems to interact with one another and exchange information according to a prescribed manner in order to achieve predictable results.[33] Interoperability between users is divided into three categories with each

32. Cognitive Radio NPRM at ¶ 76.

33. Public Safety Wireless Advisory Committee, *Final Report of the Public Safety Wireless Advisory Committee to the Federal Communications Commission*, Reed E. Hundt, Chairman, Federal Communications Commission and Larry Irving, Assistant Secretary of Commerce for Communications and Information, at 547 (September 1996) ("PSWAC Final Report").

having specific characteristics: day-to-day interoperability, mutual aid interoperability, and task force interoperability. The SAFECOM Program, managed by the Department of Homeland Security, issued a statement of requirements for public safety wireless communications and interoperability that delineates many public safety wireless operational scenarios.[34]

There are more than 18,000 law enforcement agencies and over 35,000 fire and emergency medical service agencies across the United States.[35] Due to the fragmented nature of this community, most public safety communications systems are individual systems that do not easily communicate with one another or facilitate interoperability. Federal, state, and local public safety communication systems operate in ten discrete bands ranging from 30 MHz to 869 MHz and employ a number of different air-interface protocols.[36] As a result of the fragmentation of frequency bands and air-interface standards, multiple agencies converging on a single incident often cannot communicate with each other using their radio systems. SDR and eventually CR promises to be the best long-term interoperability solution. The real need for a public safety officer, when responding to any situation, is to carry a radio that offers the ability to communicate with whomever he or she needs in real-time. That need often must be supported radio-to-radio without the use of infrastructure for on-scene use at many incidents (e.g., the use of portables). As already demonstrated by companies such as Thales and Vanu Inc., SDR offers the potential of providing a multi-band platform that supports a number of different public safety

---

34. The SAFECOM Program, Department of Homeland Security, *Statement of Requirements for Public Safety Wireless Communications and Interoperability Version 1* (March 10, 2004). SAFECOM was established to serve as the umbrella program within the federal government to help local, tribal, state, and federal public safety agencies improve public safety response through more effective and efficient interoperable wireless communications.

35. National Institute of Justice Journal, *Can We Talk? Public Safety and Interoperability Challenge*, at 18 (April 2000).

36. Air-interface is a radio-to-radio signal path defined in terms of access method, modulation scheme, voice-coding method, channel rate, and channel data format.

waveforms.[37] Equipping a field officer with a radio that supports the waveforms of agencies in that geographic area, along with a common national interoperability waveform, would enable that officer to have direct interoperability without the need for enabling infrastructure. SDR also offers the ability to download software of existing waveforms and supports forward migration to new technologies with new waveforms.

SDR is not yet an on-the street reality. Through a contract with DOD, Thales has developed the portable Mulitband Inter/Intra Team Radio (MBITR) that is not yet type-certified for public safety use.[38] Likewise, Vanu has demonstrated the Universal Communicator, a multi-mode, multi-band radio operating on a Compaq iPAQ platform.[39] Both require added waveforms to be of significant benefit to the user community, though they have proven the SDR concept is viable. The SDR Forum[40] is also in the process of forming a special interest group targeted at public safety users.[41]

Even with the progress in SDR technology in satisfying the requirements of public safety users, there are still significant technology hurdles that have yet to be overcome. The development of a public safety portable subscriber set is hindered by a number of technology requirements, including battery capacity, antenna development, and physical form factor. SDR

---

37. A waveform is the software package that defines the air interface and protocols necessary to enable communications using a particular technology. Project 25 Phase I, M/A-COM, EDACS, and Motorola SmartNet are all examples of waveforms that could be supported on an SDR platform.

38. The MBITR operates in the 30-512 MHz frequency range and supports amplitude and frequency modulation.

39. The Universal Communicator operates in the 100 to 475 MHz frequency range and can interoperate with multiple radio systems by touching various icons on the screen. It is configured to support analog frequency modulation and the Project 25 digital standard.

40. The SDR Forum is an international, non-profit organization dedicated to promoting the development, deployment, and use of SDR technologies.

41. The special interest group is charged with involving vendors and public safety organizations in the SDR forum's

processors and broadband power amplifiers require significant power. Public safety users require a battery that will support a radio for shifts that routinely extend 12 hours. Currently, multi-band antennas are physically too large to carry if they have to support a very wide range of frequency bands. All of the hardware, including an appropriate battery, must fit in an easy-to-carry package with an appropriate form factor that supports ease of use. Finally, the overall product must be affordable. While agencies may be willing to pay a premium for the features provided, all are constrained by today's limited public safety budgets.[42] Many of these challenges track those identified by the PSWAC when it considered SDR as a possible solution to the public safety interoperability problem.[43]

In addition to the technical issues identified above, issues related to the licensing of intellectual property (e.g., patents) could be another impediment to fielding a useful SDR product for use by public safety entities. Use of the major public safety waveforms, with the exception of analog frequency modulation, involves technology licensing issues. These issues will require negotiations with the license holders that could introduce major delays in bringing SDR products to the marketplace and involve added cost to the customer.[44]

The communications equipment used by public safety agencies typically operate within one of ten discrete radio frequency bands and use various air-interfaces. The lack of interoperability is the most significant problem contained in after action reports from major

---

initiatives to promote development of SDR technologies.

42. Mobile Radio Technology, *Software Defined Radio: The interoperability solution?*, at 40 (November 2003) ("MRT Magazine Article").

43. PSWAC Final Report at 239.

44. MRT Magazine Article at 40.

public safety incidents. Arguably, SDR and eventually CR technologies promise to be the best long-term interoperability solution, with the potential to provide the field officer with a belt-worn subscriber unit. As with any new technology, introduction will be slow and the initial products will be expensive. However, the benefits obtained from the technology will eventually drive demand up and cost down. The Commission's Rules are not limiting the use of SDR to facilitate the interoperability between public safety systems. Although a great deal of work has been done since PSWAC identified SDR as a potential solution to the public safety interoperability problem, technical, legal, and cost issues need to be resolved before the full benefits of SDR can be realized.

VIII. MESH NETWORKS OPERATING AT HIGHER FREQUENCIES WILL REDUCE INTERFERENCE TO OTHER RADIO SERVICES AND CAN FACILITATE BROADBAND COMMUNICATIONS.

The Commission seeks comment on the application of mesh networking technology and possible changes needed to facilitate the use of this technology.[45] Specifically, how mesh network technology might serve the Commission's efforts to facilitate broadband communication services to consumers and any rule changes that might be necessary. The Commission seeks comment on the impact that mesh networks will have on the aggregate interference to licensed services.[46] The Commission also seeks comment on the ability of mesh network capabilities to "self heal" to improve the reliability of operations.[47]

In mesh networks, sophisticated digital modulation schemes, traffic routing algorithms, and multi-hop architectures are employed that use minimal transmission power to increase data

45. Cognitive Radio NPRM at ¶ 77.

46. *Id.* at ¶ 79.

47. *Id.* at ¶ 80.

throughput over greater distances. With mesh networks, any node within the network can send or receive messages and can relay messages for any one of its neighboring nodes, thus providing a relay process where data packets travel through intermediate nodes toward their final destination. In addition, automatic rerouting provides redundant communication paths through the network should any given node fail. This ability to reroute across other links not only provides increased reliability, but also extends the network's reach. This resilient, self-healing nature stems from mesh networks distributed routing architecture where intelligent nodes make their own routing decisions, avoiding a single point of failure. The self-healing aspects of mesh networks are discussed in more detail in Appendix D.

The IEEE 802.15.4 standard specifies a physical layer that could be used for mesh networking devices. The physical layer defines parameters such as the frequency, bandwidth, transmit power, and receiver sensitivity. Given the large number of transmitters in a mesh network that can be operating simultaneously, there is a potential risk for aggregate interference to authorized radio services. Currently, the IEEE 802.15.4 standard is implemented in the 902-928 MHz and 2400-2483.5 MHz Industrial, Scientific, and Medical (ISM) bands. Because these bands are used primarily by unlicensed devices, there is no impact on federal government operations if mesh network operations are implemented in them. Before mesh networks can be implemented in the 5725-5850 MHz ISM band, however, technical analysis similar to those for the U-NII devices in the 5 GHz band would have to be performed to assess the potential impact to government radars that also operate in this band.

Since the length of communications paths for mesh network devices are short by design, it may be possible to implement this technology at higher frequency bands where propagation losses are greater. Using higher frequencies would limit the range of interfering signals within

the mesh network and substantially increase frequency reuse. This is discussed in more detail in Appendix D.

Another aspect of mesh networks is that the capacity of the mesh increases as more nodes are added. It may also be possible to use technologies for the mesh nodes such as ultrawideband (UWB), which has the potential to support data rates of 100 mega bits per second or more at short distances. The ability of mesh networks to support higher data rates is discussed in greater detail in Appendix D.

A mesh network allows nodes or access points to communicate with other nodes without being routed through a central switch point, eliminating centralized failure, and providing self-healing and self-organization. NTIA believes that the short-range characteristics of mesh networks lend themselves to using higher frequencies. Higher frequencies will become continually more attractive as RF devices become cheaper and better; denser device deployments such as mesh networks reduce the required path length; and demand for wide bandwidths and frequency reuse increases. Operating at higher frequencies will also reduce the potential for aggregate interference to other radio services. NTIA believes mesh networks that have the capability to increase capacity as the number of nodes increases can deliver broadband data rates to support high-speed data, video and voice applications.

IX. GEO-ENCRYPTION TECHNIQUES CAN BE USED IN CONJUNCTION WITH EXISTING ENCRYPTION TECHNIQUES TO PROVIDE PROTECTION OF OVER-THE-AIR SOFTWARE DOWNLOADS.

The Commission seeks comment on whether any modifications are necessary to the security and authentication requirements in the rules. Specifically, the Commission seeks comment on whether the current rules provide adequate safeguards against unauthorized

modifications to SDRs.[48]

Location-based encryption or geo-encryption refers to any method of encryption in which ciphertext can be decrypted only at a specified location.[49] If someone attempts to decrypt the data at another location, the decryption process fails and reveals no details about the original plaintext information. The device performing the decryption determines its location using some sort of location sensor, such as a GPS receiver. Location-based encryption can be used to ensure that data cannot be decrypted outside of a particular facility (*e.g.*, the headquarters of a government agency or corporation). Alternatively, it may be used to contain access to a broad geographic region. Time and space constraints can also be placed on the decryption location. Appendix E describes one implementation of geo-encryption that builds on established security algorithms and protocols.

Geo-encryption has the potential to support both fixed and mobile applications and a variety of data-sharing and distribution policies. Depending on individual implementations, it can also provide strong protection against location spoofing. NTIA believes that geo-encryption techniques can be used in conjunction with existing encryption techniques to provide protection of over-the-air software downloads. NTIA recommends that the Commission explore the benefits and possible implementation of geo-encryption techniques as part of future rulemaking proceedings on CR and SDR technologies.

48. Cognitive Radio NPRM at ¶ 94.

49. Geo Intelligence, *GPS-Based Geo Encryption*, at 26 (Winter 2003).

X. THE INITIAL IMPLEMENTATION OF UNLICENSED COGNITIVE RADIO TECHNOLOGY SHOULD BE LIMITED TO THE INDUSTRIAL, SCIENTIFIC, AND MEDICAL FREQUENCY BANDS AND THE FREQUENCY BANDS TRANSFERRED FROM THE FEDERAL GOVERNMENT.

The Commission seeks comment on whether higher power operation should be permitted for Part 15 devices. For example, the Commission questions whether higher power unlicensed device operation should be permitted under Section 15.209 of the Commission's Rules.[50]

Section 15.209 of the Commission's Rules permits unlicensed device operation at specified radiated emission levels, in almost any frequency band, other than the television broadcast and certain designated restricted frequency bands.[51] The restricted frequency bands include bands used to support safety-of-life functions, such as aeronautical radionavigation, and bands employed by radio services that must function, as a nature of their operation, using extremely low received signal levels. However, there are many frequency bands used by critical government and non-government radiocommunication systems that are not included in the restricted frequency band list but also require protection. Examples of these critical systems include the Federal Aviation Administration's Terminal Doppler Weather Radar;[52] the DOD systems used to provide tracking, telemetry, and control of all military satellite systems; the National Aeronautics and Space Administration's Tracking and Data Relay Satellite System; the Department of Transportation's Intelligent Transportation System;[53] commercial cellular and personal communication service (PCS) systems; point-to-point microwave systems used to

50. Cognitive Radio NPRM at ¶ 41.

51. In the restricted frequency bands, only spurious and unintentional emissions from unlicensed devices are permitted.

52. The Terminal Doppler Weather Radar provides quantitative measurements of gusts fronts, wind shear, microbursts, and other weather hazards for improving the safety operations at major airports.

53. The Intelligent Transportation System Dedicated Short Range Communication Service is used to support public

support the Nation's critical infrastructure;[54] and land mobile communications systems used to support state, local, and federal public safety. These critical government and non-government systems span the frequency range of 100 MHz to 7000 MHz.

The low radiated emission levels currently permitted under Section 15.209 are the primary factor that facilitates sharing between unlicensed devices and the licensed radiocommunication systems. Before an increase in the power level for unlicensed devices can be considered, operational parameters (including sharing criteria) of both the licensed services and the proposed unlicensed uses are required to adequately determine the necessary technical characteristics of the CR technique to be employed. An example of an appropriate methodology for conducting the analyses to define the characteristics of the CR technique can be seen by examining the U-NII rulemaking proceeding. The analyses used to determine appropriate thresholds for use by U-NII devices employing DFS took into account the technical characteristics of the radar transmitter and receiver (*e.g.*, antenna gain patterns, bandwidth, scan/tracking rate) as well as the technical characteristics of the unlicensed device proposed for the radio local area networks (RLAN). For this specific unlicensed device application, the analysis was used to determine combinations of transmit power, antenna gain, bandwidth, and measurement time interval that would allow successful sharing between unlicensed RLANs and radar systems. Similar analyses would need to be conducted for each frequency band being considered, each higher-powered unlicensed application, and the CR techniques to be employed to facilitate sharing. Each analysis would be unique due to differing technical characteristics of the various licensed and various unlicensed device applications, as well as the differing

---

safety communications on the Nation's highways.

54. Fixed point-to-point microwave systems are used by public safety, railroads, and the energy and water

propagation characteristics in each frequency band.

The effectiveness of the CR technique employed by the unlicensed device to facilitate sharing with licensed users will be dependent on the licensed service operating in the band. For example, DFS techniques hold promise for sharing with radar systems or with other radio services where the transmitter and receiver are at the same location and where the propagation path from the DFS-equipped unlicensed device back to the transmitter is the same as the path from the transmitter to the DFS-equipped unlicensed device. However, for sharing with point-to-point microwave systems, where the transmitter and receiver are typically separated by tens of kilometers, the hidden transmitter problem can exist.[55] For sharing with point-to-point microwave systems, geo-location CR techniques used with an on-line location database may be more appropriate. Detection techniques such as DFS are also not very effective when the licensed user's signal operates below the noise floor, for example spread spectrum systems.

The Commission's proposal to permit higher-powered unlicensed device operation when CR sensing techniques are employed includes three ISM frequency bands: 902-928 MHz, 2400-2483.5 MHz, and 5725-5850 MHz. NTIA agrees with the Commission's current proposal to initially limit higher-powered unlicensed device employing CR sensing techniques to the 902-928 MHz and 2400-2483.5 MHz bands. Because these frequency bands are primarily used by unlicensed devices that must accept interference from other unlicensed devices, compatibility analyses with government systems are not necessary. However, in the 5725-5925 MHz frequency band, the DOD operates fixed, transportable, and mobile radar systems and analyses

---

industries.

55. In the hidden transmitter problem, if a spectrum sensing equipped unlicensed device is blocked from receiving the transmitted point-to-point signal (*e.g.*, shielded by local terrain features) it will be permitted to transmit, possibly causing interference to the point-to-point receiver that is located close to the spectrum sensing equipped unlicensed device.

will have to be performed to assess the potential impact that the Commission's proposal will have on these critical systems.

If the Commission is contemplating expanding the implementation of higher-powered unlicensed device operations employing CR techniques, NTIA recommends that the Commission consider the frequency bands transferred from federal government to private sector use.[56] The transferred frequency bands represent spectrum that at this time has limited government or commercial use. In an on-going rulemaking proceeding, the Commission is already examining the implementation of CR techniques in the 3650-3700 MHz band to facilitate sharing between higher-powered unlicensed device and licensed radio services (radar systems and satellite earth station receivers).[57]

XI. SECONDARY SPECTRUM MARKET ACTIVITIES PROMISE TO INCREASE SPECTRUM EFFICENCY BY FOLLOWING CHANGING DEMAND.

The Commission seeks comment on technical methods that might be used to provide information necessary for leasing of spectrum and how a device would enforce the terms of the lease. Specifically, the Commission requests comment on whether they could reduce the uncertainties that may inhibit leasing transactions by encouraging voluntary technical standards for access to a licensee's spectrum. The Commission also requests comments on what approaches to facilitate leasing transactions could best achieve the goals of the flexible and

56. In accordance with the requirements of Title VI of the Omnibus Budget Reconciliation Act of 1993 and the Balanced Budget Act of 1997, 247 MHz of federal government spectrum have been identified for transfer to the private sector.

57. *Additional Spectrum for Unlicensed Services Below 900 MHz and in the 3 GHz Band; Amendment of the Commission's Rules with Regard to the 3650-3700 MHz Government Transfer Band,* Notice of Proposed Rulemaking, ET Docket No. 04-151, ET Docket No. 02-380, ET Docket No. 98-237, FCC 04-100, 2004 FCC LEXIS 2071, at ¶¶ 64-68 (2004).

market-driven policies for spectrum leasing.[58]

NTIA has, for several years, supported the development of secondary markets as a means of promoting efficient use of spectrum.[59] To promote these secondary markets, it is important to maximize as much as possible the flexibility for accommodating these markets. In permitting secondary market activities, the Commission should not over-regulate the leasing process or require secondary user registration or lessee filings. NTIA advocates that licensees retain ultimate responsibility for any activity under their lease. By making licensees responsible, the Commission will have a mechanism for ensuring its rules are followed. NTIA would suggest, however, that the Commission impose certain minimum criteria for licensees to follow in entering into lease arrangements to ensure appropriate intervention in the event of misuse by the lessee. The Commission should require licensees to maintain on file the lease agreement with availability to the Commission upon request; notify the Commission upon agreement to a lease; maintain on file contact information for any secondary users of their spectrum; have contractual authority to terminate the lease in response to a violation; approve any subsequent sublease; and assist in enforcement of the lease conditions and administrative regulations.

Making the licensee responsible for any use within the scope of its license will provide incentives for the licensee to construct the appropriate covenants, indemnifications and limitations within its contract to ensure appropriate use by the lessee. These basic principles of minimum regulation of secondary markets should be extended to the application of CRs to facilitate the establishment of secondary markets.

---

58. Cognitive Radio NPRM at ¶ 50.

59. Letter from Nancy J. Victory, Assistant Secretary for Communications and Information, National Telecommunications and Information Administration, to the Honorable Michael K. Powell, Chairman, Federal Communications Commission (March 7, 2002).

The Commission should consider permitting the deployment of beacon signals and control and communication links that would aid CR systems to identify spectrum that is available to the lessee. These beacon signals and communication links would be restricted to the same spectral and geographical constraints as those of the licensee. The Commission should allow preemption of the lessee use of the spectrum by the licensee subject to lease agreements. Licensees in cooperation with lessees operating in the same or similar bands should also be encouraged to develop voluntary standards for lessee equipment and operations as required.

NTIA supports the actions taken by the Commission to remove regulatory barriers to the development of secondary markets. These flexible policies will continue the evolution toward greater reliance on the marketplace to expand the scope of available wireless services. Because CRs can play an enabling role in the establishment of secondary markets, the development of CR technology should also have similar, minimum regulatory constraints.

XII. HIGH-SPEED DIGITAL-TO-ANALOG CONVERTERS THAT ARE MARKETED AS PART OF RADIO SYSTEMS SHOULD BE REGULATED AS SOFTWARE DEFINED RADIOS OR COGNITIVE RADIOS UNDER THE APPROPRIATE SECTION OF THE COMMISSION'S RULES.

The Commission seeks comment on whether there is a need to restrict the mass marketing of high-speed, digital-to-analog converters (DAC) that could be diverted for use as radio transmitters and whether it can do so without adversely affecting other uses of such computer peripherals or the marketing of computer peripherals that cannot be misused.[60]

DACs are finding increased use in modern communication systems and will be a key element in the implementation of SDR and CR technologies. DAC circuits can be used in local oscillators, clock generator blocks, and wideband modulator circuits. The sources of spurious

60. Cognitive Radio NPRM at ¶ 92.

emissions generated by DACs can generally be attributed to the nonlinearities associated with the non-ideal static and dynamic transfer functions of the DAC.[61] Spurious emissions from the DAC can be categorized into three types: spurious emissions caused by direct circuit nonlinearities within the DAC; harmonically related spurious emissions caused by non-ideal switching characteristics of the DAC; and spurious emissions caused by noise coupling effects that can be harmonically or non-harmonically related.[62]

The marketing of high speed DACs and the software to make them interact could undermine the Commission's present equipment authorization program at the risk of increasing interference to legitimate spectrum users. This could occur because these devices would not be subject to the normal equipment authorization requirements. This is not presently a problem, but the Commission is considering steps that can be implemented now to help ensure that this scenario does not become a serious problem.

NTIA commends the Commission for addressing the potential problems of emitters that could fall outside of the present regulatory structure as part of this proceeding. The issue of the blurring of applicability of specific rule sections as technology advances is but one indicator of the problems facing the regulatory community in trying to keep pace with technology evolution. While trying to avoid undue burden on the introduction of innovative technology, the Commission clearly has the responsibility to regulate spectrum use such that adverse effects to other authorized users does not occur. The Commission has expressed specific concern that high speed DACs might be used with high processing speed personal computers to create software-controlled RF signal sources that can be used as transmitters.

---

61. RF Design, *Sources of Spurious Components in a DDS/DAC System,* at 28 (April 1998).

62. *Id.*

NTIA believes that there is no reason to regulate component parts such as DAC integrated circuits and any regulation that would likely stifle their use should be avoided. NTIA also believes that a radio transmitter consists of a means to generate, amplify, and radiate a signal into the environment. A DAC add in card alone does not possess this capability, and thus should not be subject to regulation as a radio transmitter under the Commission's rules. If a DAC is coupled with an amplifier and antenna, with intent to radiate into the environment, then it should be considered a SDR or CR and should be regulated under the applicable section of the Commission's rules. NTIA recommends as potential consumer applications of DAC based RF signal sources become better understood, that the Commission should consider revisiting their regulations.

XIII. THE COMMISSION SHOULD CONSIDER REQUIRING PROTECTION PROFILES AS PART OF THE EQUIPMENT CERTIFICATION PROCESS FOR SOFTWARE DEFINED RADIOS.

The Commission seeks comment on whether any modifications are necessary to the security and authentication requirements in their rules. Specifically, the Commission seeks comment on whether the current rules provide adequate safeguards against unauthorized modifications to SDRs. Comments are also sought on what should happen in the event that reasonable security methods are ultimately broken and what responsibilities do the manufacturers have if accepted industry standards for security are followed.[63]

The Commission's Rules require that manufacturers take steps to ensure that only software that is part of an approved hardware/software combination can be loaded onto an SDR.[64] The software must not allow the user to operate the transmitter with frequencies, output

63. Cognitive Radio NPRM at ¶ 94.

64. *See* 47 C.F.R. § 2.932(e).

power, modulation types or other parameters outside the range of those that were approved. Manufacturers may use authentication codes or any other means to meet these requirements, and must describe the methods in their application for equipment authorization. In adopting these requirements, the Commission stated that it may have to specify more detailed security requirements at a later date as SDR technology develops.[65]

NTIA shares the concerns raised by the Commission regarding the adequacy of the current software security requirements. Recurring media reports of security flaws in commercial software packages and operating systems indicate that software based security mechanisms in SDR could be vulnerable. Changes to the Commission's Rules that require the use of specific industry standard security measures would help to remove some ambiguity that exists in how security is implemented and how secure these measures must be. To address problems with security, the SDR Forum has written a document on the requirements for software downloads that reconfigure the RF characteristics of a radio.[66] This document describes the security requirements for commercial wireless systems to ensure that malicious code cannot be downloaded and activated. The security measures are divided into six generic categories: Trusted System Operator, Authentication, Authorization, Integrity, Privacy, Non-Repudiation, and Auditing.[67] All of these general security requirements are also requirements for the more specific challenges of SDR security. The SDR Forum has also developed security threat scenarios and an SDR security threat model to address the different categories of threats to

65. *Inquiry Regarding Software Defined Radios*, Report and Order, ET Docket No. 00-47, 16 FCC Rcd 17373, 13383 (2001).

66. SDR Forum, Document Number SDRF-02-A-007-C0.00, *Requirements for Radio Software Download for RF Reconfiguration* (November 13, 2002).

67. *Id.* at 29.

downloaded software that reconfigures the RF parameters.[68]

The SDR Forum is also considering Protection Profiles as a requirement for SDRs. A Protection Profile is an implementation independent statement of security requirements that is shown to address threats that exist in a specified environment.[69] A Protection Profile would be appropriate for a consumer group that wishes to specify security requirements for an application type. Protection Profiles are now becoming a standard requirement for the Common Criteria, which is the international mechanism for certification and accreditation of security devices.[70]

The main security issue that have been identified include who has the authority to control the reconfiguration of the communications equipment, protection of the reconfiguration signaling, privacy of the reconfiguration information,[71] the correctness and availability of information on which the reconfiguration is based, and secure download of software required for reconfiguration, and issues related to the radio emission and associated conformance requirements of radio equipment. NTIA is concerned about the regulatory implications associated with downloaded software that can reconfigure the radio functionality, which includes such parameters as frequency, power, and modulation. The SDR Forum, which represents a large cross section of national and international organizations, has made a great deal of progress in addressing the areas of security, authentication, and protection of unauthorized modifications to SDRs. NTIA understands the Commission's reluctance to adopt specific security requirements because this may constrain the development SDR technology. From the federal

---

68. *Id.* at Appendix A.

69. Protection Profiles are registered through national processes.

70. More information is available at http://www.commoncriteria.org/protection_profiles/pp.html.

71. For example, information on current configuration of a user's equipment.

agencies' perspective, however, NTIA believes that the acceptance of SDR, and eventually CR technologies, hinges on assurances that the operating parameters that can impact electromagnetic compatibility with other systems are protected from malicious attacks. NTIA recommends that as a long-term goal of addressing security issues related to SDR and CR technologies, the Commission consider requiring Protection Profiles as part of the equipment certification.

XIV. THE REQUIREMENT FOR APPLICANTS TO PROVIDE A COPY OF THEIR SOFTWARE AS PART OF THE CERTIFICATION PROCESS FOR SOFTWARE DEFINED RADIOS SHOULD BE ELIMINATED.

The Commission proposes to delete the requirement that applicants supply a copy of their radio software upon request. In its place the Commission proposes to add a less burdensome requirement that applicants supply a description and flow diagram of the software that controls the radio operating parameters.[72]

NTIA agrees with the Commission that examination of software is not an effective means of identifying where unauthorized software changes have been made in an SDR. NTIA believes that the Commission's requirement that certified devices must comply with their applicable technical rules is sufficient to safeguard against unauthorized equipment modifications. Thus, NTIA agrees with the Commission's proposal to eliminate the existing requirement for applicants to provide copies of their software as part of the certification process for SDRs.

72. Cognitive Radio NPRM at ¶ 86.

XV. MANUFACTURERS SHOULD ONLY BE REQUIRED TO DECLARE THEIR DEVICES AS A SOFTWARE DEFINED RADIO IF THE DEVICE IS REMOTELY PROGRAMMABLE AND HAS HARDWARE CAPABLE OF TRANSMITTING IN THE RESTRICTED FREQUENCY BANDS OR IN FREQUENCY BANDS ALLOCATED TO THE FEDERAL GOVERNMENT ON AN EXCLUSIVE BASIS.

The Commission requests comments on the need for a requirement that manufacturers declare certain equipment as SDRs, including the benefits of such a requirement in reducing interference and its possible burden on manufacturers. Specifically, the Commission seeks comment on the type of device to which this requirement should apply, including how the rules should distinguish between transmitters that must be identified as SDRs.[73]

NTIA agrees with the concerns raised by the Commission regarding an SDR's ability to modify its parameters. Operating outside of the parameters approved under the rules for that device, would increase the potential for interference to other authorized radio services.[74] Issues related to unauthorized users having the capability to modify or reprogram an SDR to operate outside of its allowable parameters continues to be a concern to many of the federal agencies. Requiring manufacturers to declare a device as being an SDR would require that the security mechanisms must be incorporated, which provides some assurance that unauthorized users cannot modify the parameters of SDRs. This would reduce the interference risk to other radio services.

The definition for SDR adopted by the Commission is extremely broad and covers devices in which parameters such as frequency and modulation type are determined by software.[75] The problem is that the definition of SDR could also apply to non-government

---

73. Cognitive Radio NPRM at ¶ 88.

74. *Id.* at ¶ 87.

75. A software defined radio is one that includes a transmitter in which the operating parameters of frequency

private land mobile radios and most commercial PCS base stations, which were not intended to be included under the rules for SDR. The Commission's current rules do not require manufacturers of SDRs to declare them as such when applying for equipment authorization. A device that is not declared as an SDR does not have to comply with the software security requirements that are designed to ensure that only authorized software can be loaded.[76] NTIA recognizes the potential problem that can be encountered by applying the broad definition for SDR. However, there is still a potential problem with an SDR whose transmitter parameters can be changed remotely. In this situation, large numbers of transmitters could be modified simultaneously, thereby increasing the potential interference to federal spectrum users.

NTIA believes that the primary concern to federal operations would come from SDRs that are remotely programmable and have the hardware capability to transmit in the restricted frequency bands or in other frequency bands used by the federal government. NTIA believes that it would be appropriate for the Commission to require manufacturers to declare their devices as SDRs if the device is remotely programmable and has hardware that is capable of transmitting in the restricted frequency bands or in frequency bands allocated to the federal government on an exclusive basis. This would eliminate the problems associated with incorrectly classifying commercial devices, such as land mobile radio and PCS, as SDRs and provide protection to federal users.

---

range, modulation type or maximum output power (either radiated or conducted) can be altered by making a change in software without making any changes to hardware components that affect the radio frequency emissions.

76. The manufacturers of SDR devices are now required under Section 2.932(e) of the Commission's Rules to take steps to ensure that only software that has been approved with a SDR can be loaded into such a radio.

XVI. TECHNICAL ISSUES RELATED TO THE COMPLIANCE MEASUREMENTS OF UNLICENSED DEVICES THAT EMPLOY COGNITIVE RADIO TECHNIQUES MUST BE ADDRESSED PRIOR TO IMPLEMENTATION.

Since devices employing CR techniques can perform functions not envisioned at the time the current Part 15 Rules were developed, the Commission recognizes that it will be necessary to specify additional compliance measurement procedures. In the NPRM, the Commission proposes a number of specific tests applicable to the following CR techniques: interruptible radio,[77] listen-before talk,[78] and geo-location.[79] The Commission seeks comment on its proposed compliance measurement tests and whether additional tests might be necessary. The Commission also solicits public comment on whether it or an industry standards organization, such as the American National Standards Institute (ANSI), should develop the compliance measurement procedures.[80]

Currently, when Part 15 devices are certified, the output of the device is tested in response to a single or limited number of input conditions to verify that it complies with the Commission's Rules. However, for unlicensed devices employing CR techniques, it will be necessary to test the output in response to various inputs or various combinations of inputs. NTIA is currently participating in a government/industry working group that is developing compliance measurement guidelines for U-NII devices that are equipped with DFS.[81] In this case, the compliance measurements must verify the DFS detection threshold, startup and in-

77. Cognitive Radio NPRM at ¶ 103.

78. *Id.* at ¶ 105.

79. *Id.* at ¶ 106.

80. *Id.* at ¶ 102.

81. DFS is the same as the sensing or listen-before-talk techniques described in the NPRM.